BALTIMORE

global
e-security

Attribute Certificates

Lisa Pretty

VP Strategic Marketing

lpretty@baltimore.com

(650)372-5275

McLean, VA office (703)749-1406

www.baltimore.com

BALTIMORE

global e-security

Agenda

- What are Attributes?
- Handling attributes in certificates
- Attribute Certificates
- Benefits of attribute certificates
- Issuance, distribution and use
- Examples of attribute certificate applications
- Role based access control
- Using Attribute Certificates for role based access
- Questions and Answers

global e-security

Application Requirements

- Once an application knows who someone is i.e. proved authenticated
- the problem is “what are they allowed to do?” :
  - access information
  - change information
  - commit a transaction
  - spend this amount
  - cancel this transaction
  - etc.
- The solution is that the application has to understand attributes about the user

BALTIMORE

global e-security

Role/Attribute Characteristics

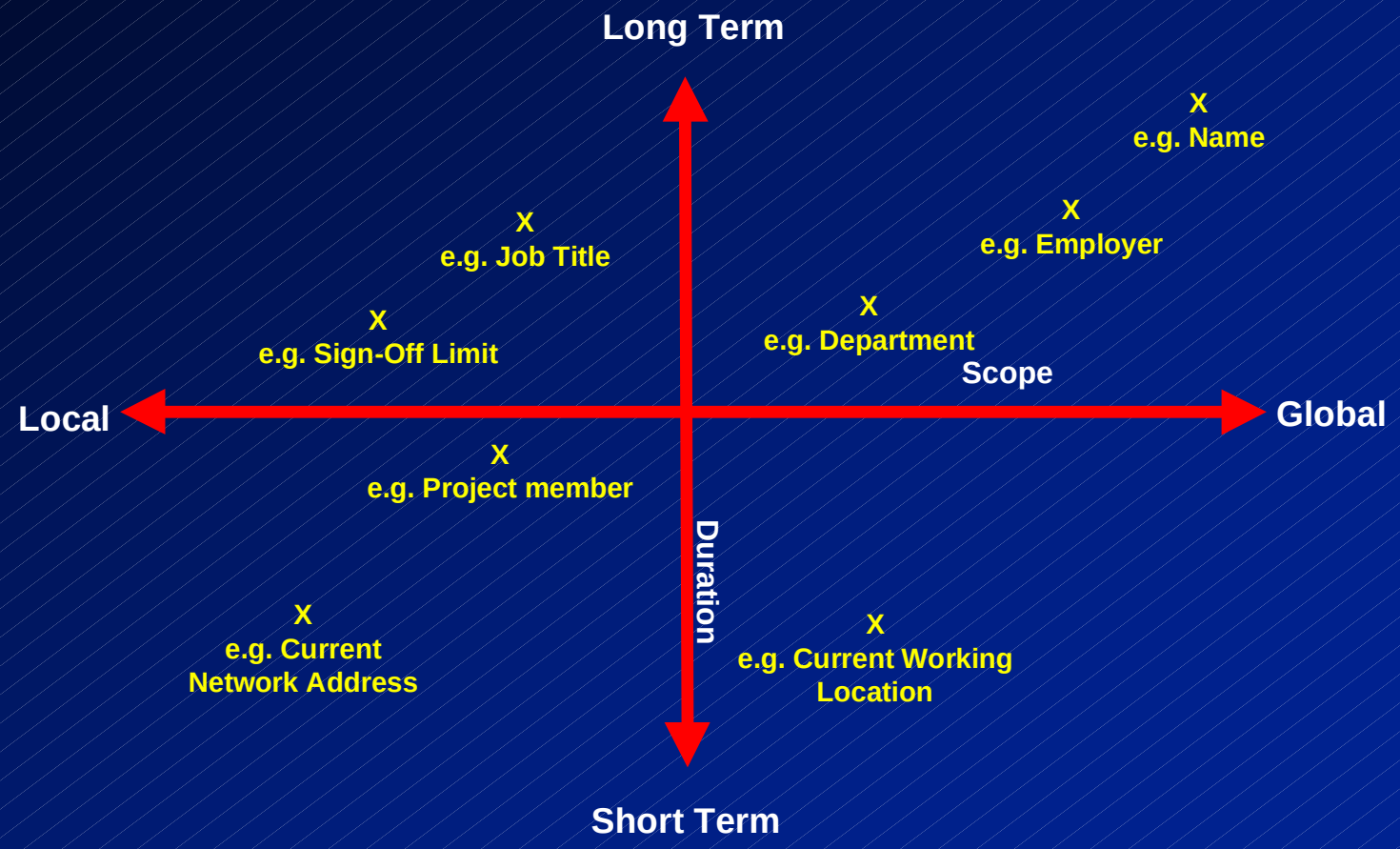
- May change frequently
  - Roles change
  - May depend on place of work on a specific day
  - May depend on time of day
- May be owned and managed by different authority to identity certificates
  - Identity certificates may be issued centrally/externally
  - Attribute information may be managed locally
- May be specific to an individual application
  - i.e. may be meaningless to another application
  - want easy management of access to applications

BALTIMORE

global e-security

www.baltimore.com

The Nature of Attributes



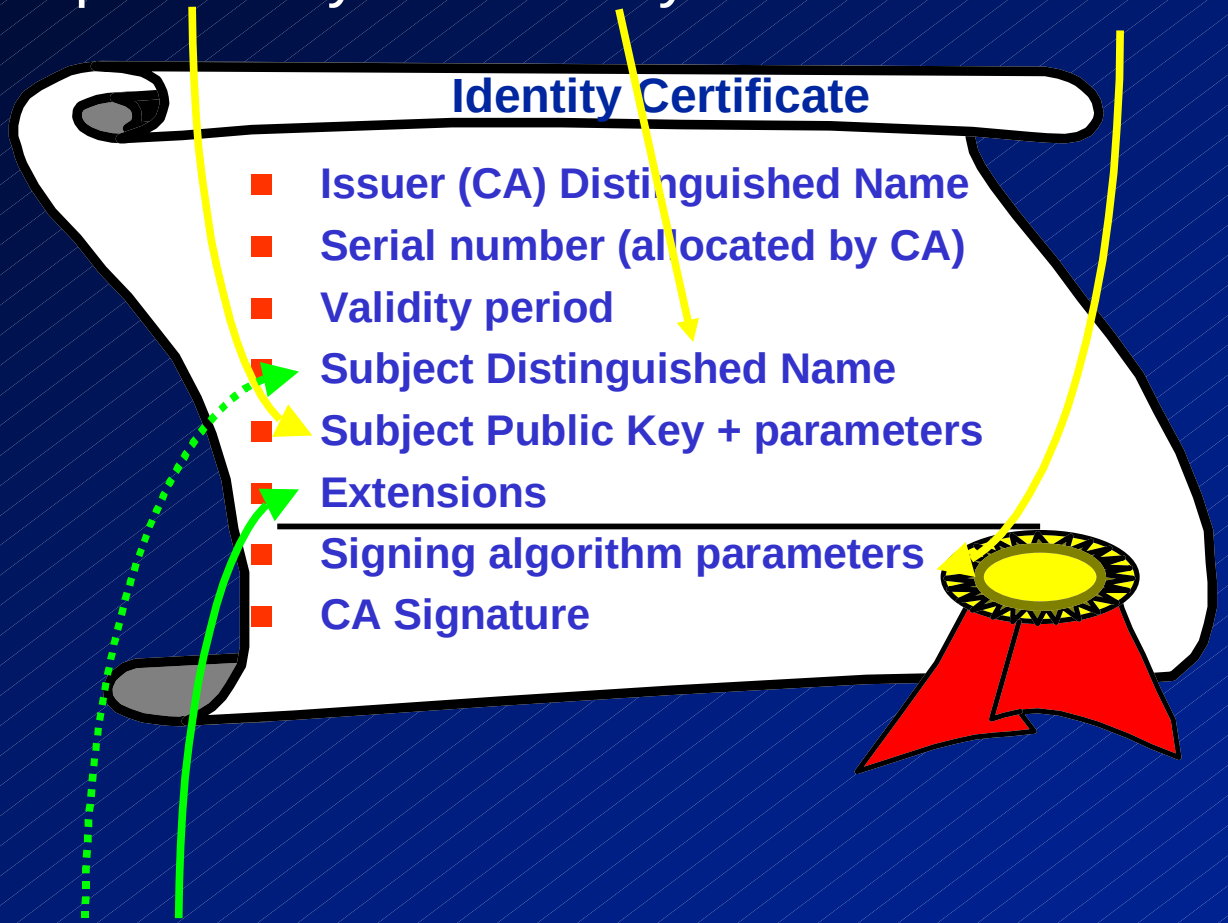
How can we support these different types of attributes?

BALTIMORE

global e-security

X.509 Certificates

Tie a public key to an entity in a trusted manner



Some attribute information can be added

www.baltimore.com

BALTIMORE

global e-security

Solution- X.509v3 with extensions?

- Private/custom extensions can be defined
- Good fit if:
  - CA/RA entity also has knowledge of roles/permissions
  - Life of attribute matches life of identity certificates
  - Applications understand custom extension (and not marked as critical so other applications can ignore)
- Otherwise it's a poor fit

BALTIMORE

global e-security

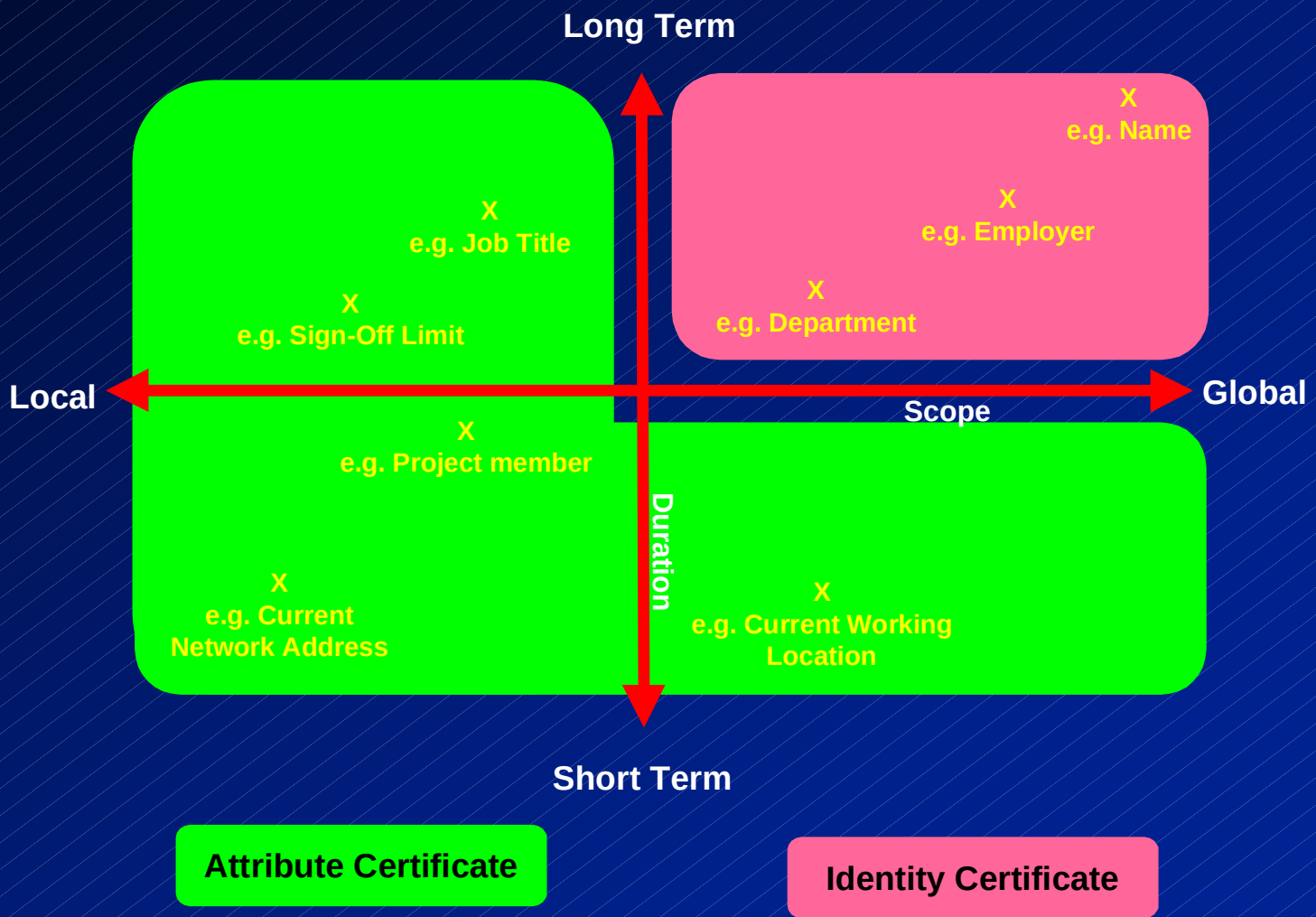
Separate Certificates

- Identity Certificate:
  - binds name and key
  - long life
- Attribute Certificate:
  - carries attribute information
  - shorter life time
  - local use - may be specific to one application
  - can have multiple attribute certificates bound to the same Identity Certificate
- Both defined in X.509

BALTIMORE

global e-security

The split between certificates



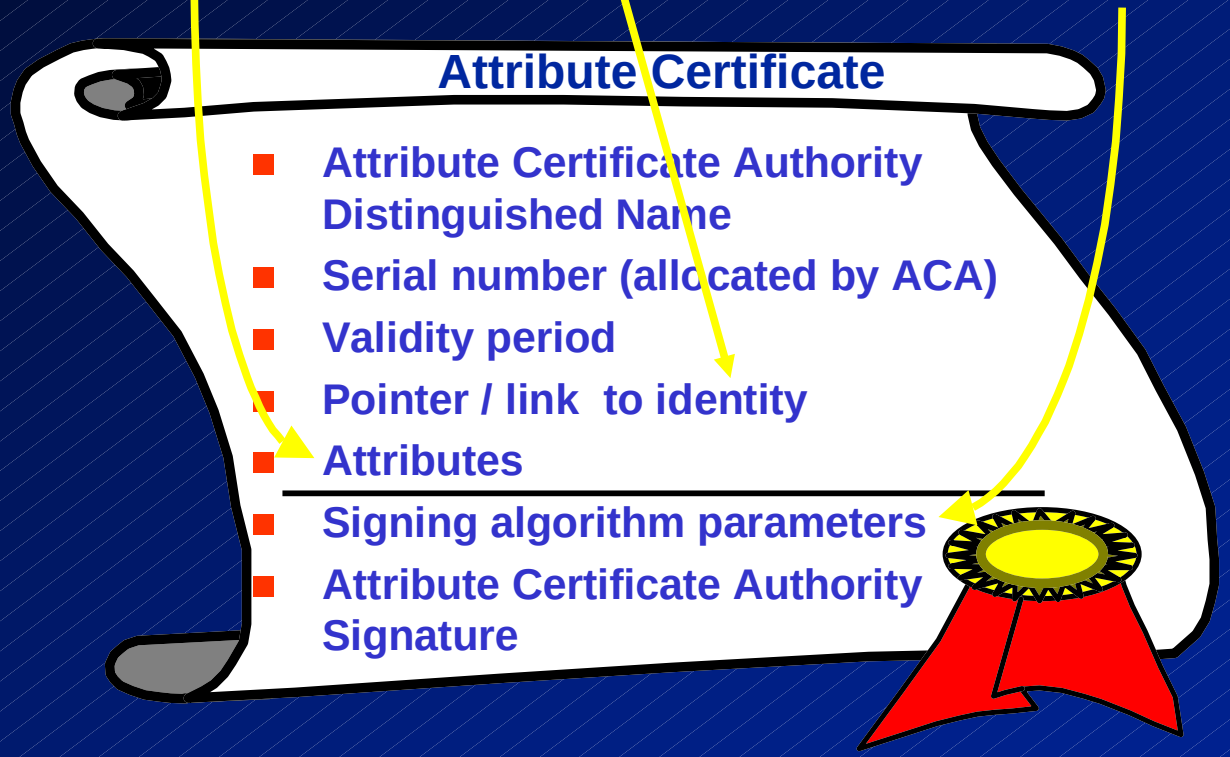
www.baltimore.com

BALTIMORE

global e-security

Attribute Certificates

Ties attributes to an entity in a trusted manner



No public key

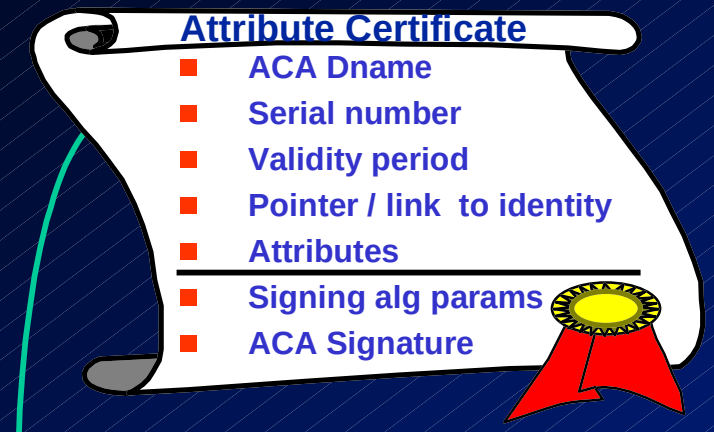
www.baltimore.com

BALTIMORE

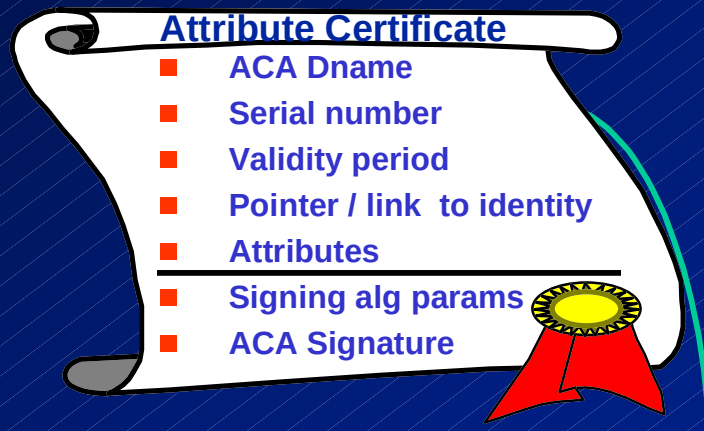
global e-security

www.baltimore.com

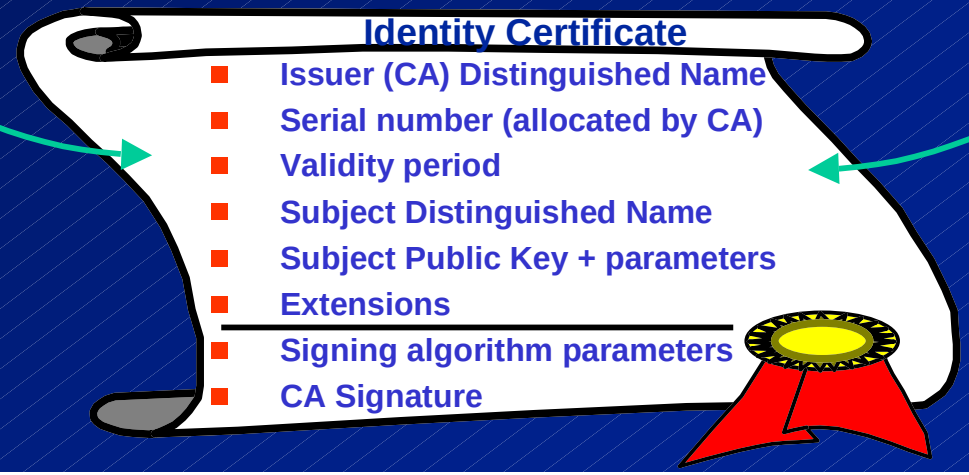
Attribute Certificates



- Issued by AC Issuer 1
- Used by applications A + B



- Issued by AC Issuer 2
- Used by applications D, E, F



BALTIMORE

global e-security

Benefits of Attribute Certificates

- Interoperability
  - Application specific information is removed from the identity certificate
- Jurisdiction
  - Attribute certificates can be issued by organization that controls the “attributes” which may not be the same as identity
- Revocation
  - Attribute certificates may have short life
- Flexibility
  - Multiple attributes per user
  - Roles/attributes change at different time intervals

BALTIMORE

global e-security

Standards and other Initiatives

- ANSI X.509 Related
  - LDAP schema for Role Based Access Control
  - TLS extensions for Attribute Certificate based authorization
- IETF draft standards not based on X.509
  - Capability Card: An Attribute Certificate in XML
  - Simple Public Key Infrastructure (SPKI) - set of four internet drafts (goal = authorization)
- Open Group
  - Open Software Foundation Distributed Computing Environment: Kerberos, Access Control Lists (ACLs) and Privilege Attribute Certificates (PAC)
- Various Access control, VPN control and role based products on the market

BALTIMORE

global e-security

Attribute for TLS authorization

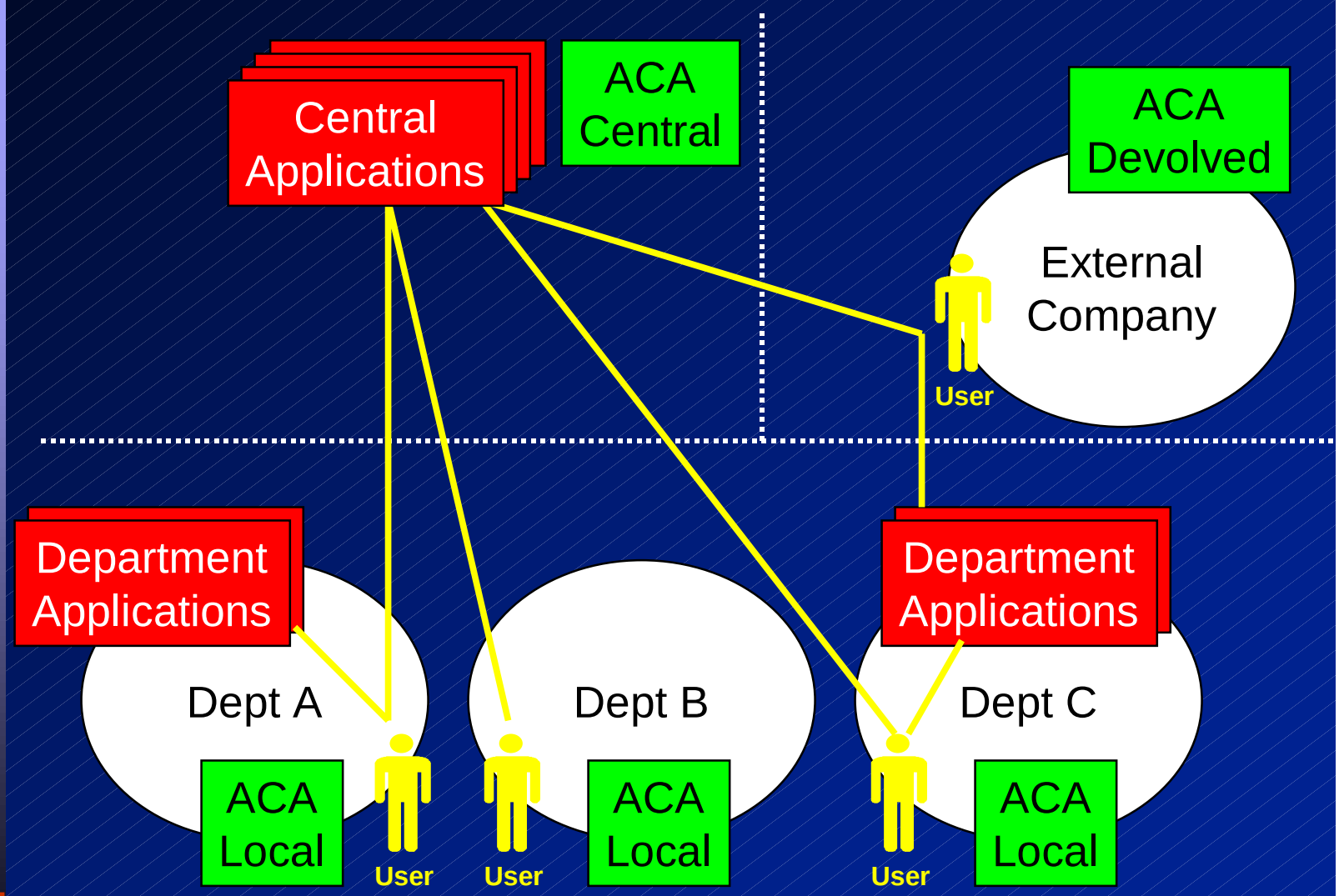
- Roles
- Groups
- Access identities
- Custom attributes
- Restrictions

www.baltimore.com

BALTIMORE

global e-security

Issuance of Attribute Certificates



www.baltimore.com

BALTIMORE

global e-security

Issuance

- Central issuance - advantages
  - Suitable for small organizations
- Local issuance - advantages
  - Simplified user authentication
  - Simplified issuance procedures
  - Reduced administration overhead
  - Greater control
  - Simpler distribution
- Devolved issuance - as per local issuance

BALTIMORE

global e-security

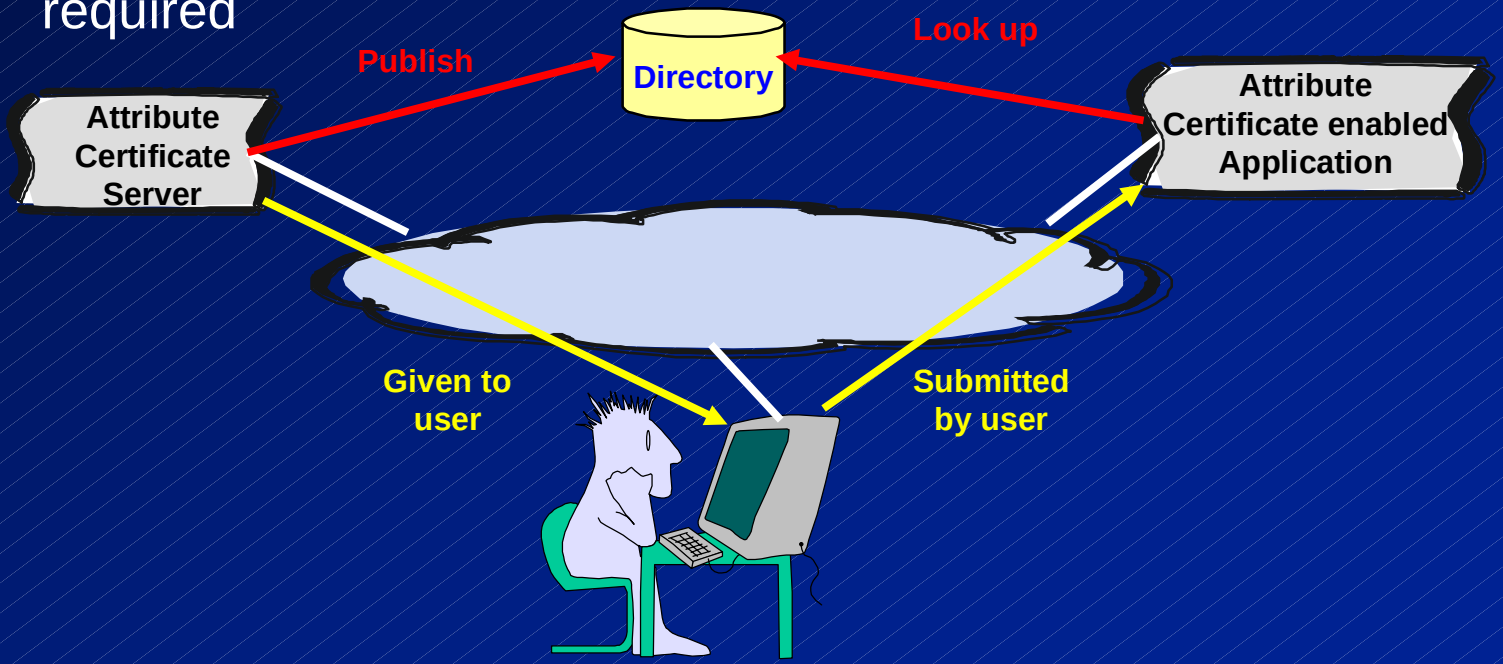
Distributing Attribute Certificates

Pull

- Mirrors X.509 identity cert model -- certificates are written to directory (e.g. X.500)
- Applications requiring attribute certificates may “pull” them as required

Push

- Users supply attribute certificate directly to application (similar to password model)
- No directory

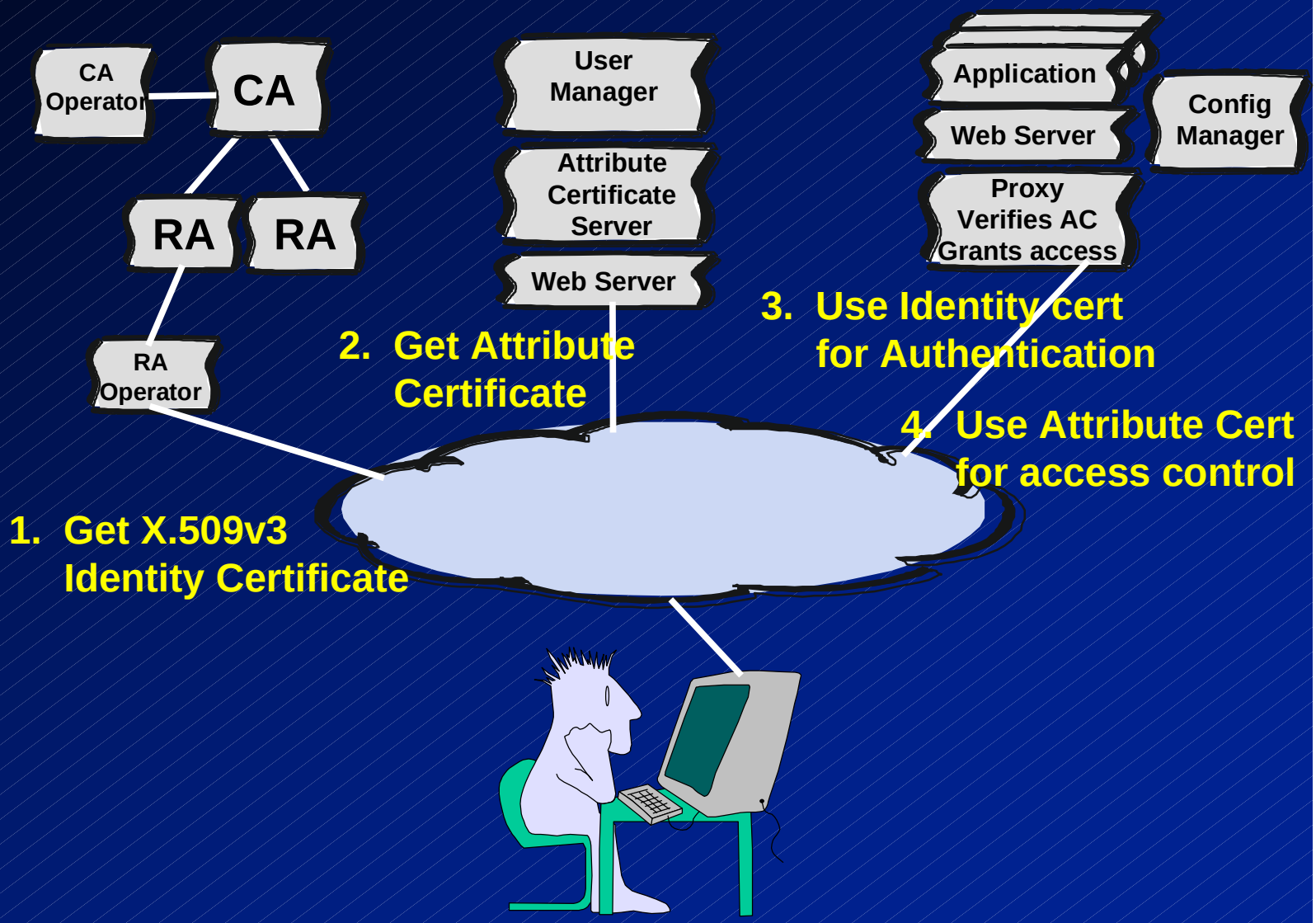


www.baltimore.com

BALTIMORE

global e-security

Using Attribute Certificates



www.baltimore.com

global e-security

Using Attribute Certificates

- Certificate (PKI) based authentication of user
  - SSL with client authentication
  - S/MIME with signature
  - Challenge response
  - Signed objects
- Check attribute certificate is linked to identity
- Check ACA is allowed
- Check ACA signature
- Extract attributes and use

BALTIMORE

global e-security

Applications

- Corporate implementation of roles and authorities for all e-business
- Control of subscription service (e.g. pay-per-view)
- Access control within a network
- Time sensitive use of resources (University Students)
- Web page access control
- etc.

BALTIMORE

global e-security

Access Control - ACL

- Access control lists
  (user id, password, permissions)
  - Difficult to maintain applications
  - Difficult to maintain user base
  - Difficult to scale
  - User may require separate details for each system
  - Have to know each user

global e-security

Access Control - Role Based

- Role Based
  - Easier to maintain applications
  - Easier to maintain user base
  - Much easier to scale
  - User may be able to use same role across multiple systems
  - Users do not have to be known

BALTIMORE

global e-security

Attribute Certs for Access Control

- Provide a secure container for attributes linked to X.509 identity certificates
- Support both push and pull models
- Support central, local and devolved issuance
- Support central and local use
- Can be specific to one application
- Can be general to many applications
- Can be very short term validity
- Can use different PKIs

BALTIMORE

global e-security

Scenario - Web Page Access Control

- Bank's web pages need access control according to a user's role within the bank
- Requirements
  - Strong user authentication
  - Role based access control
  - Local allocation of access rights but central control of Web resources. E.g. roles are assigned within each branch, but the bank Web server gives access to resources according to a user's role
  - Fine granularity of access control and flexibility in how the access rights are used

BALTIMORE

global e-security

Role, Group and Access Matrix

Page Class	Page Contents	Teller	Supervisor	Loan Officer	Branch Manager	Group
Account Management	Customer Details	✓	✓	✓	✓	
	Account Balance	✓	✓		✓	
	Credit Ratings			✓	✓	
	Credit Limits		✓		✓	
	Transaction History		✓	✓	✓	
Current Rates	Exchange Rates	✓	✓	✓	✓	
	Interest Rates	✓	✓		✓	
	Loan Rates			✓		
Branch Statistics	All Branches		✓			
	San Jose				✓	**San Jose**
	Palo Alto				✓	**Palo Alto**
Staff Details	San Jose		✓			**San Jose**
	Palo Alto		✓			**Palo Alto**

www.baltimore.com

global e-security

Benefits of using Attribute Certs

- Management of Role/Attribute information
  - Can match the business infrastructure
  - Can be independent of Identity PKI
- Attribute (role) based access control (not user based)
  - eases access control maintenance
  - eases application maintenance
  - scalability of user base
- Short term attribute certificates can help with the revocation problem
- Applications don't have to understand one another's specific attributes
  - reduces interoperability problems

global
e-security

Questions & Answers

LPretty@baltimore.com

www.baltimore.com